



Apellido: FESTINI	LU: 331/17	Hojas >	Ej.1 1	Ej.2 3	Ej.3 1	Ej.4 1	4
Nombres: SANTIAGO		Calif. >	B+	B+	B+	B	Final: A

Todas las respuestas se consideran válidas solo si están debidamente justificadas.

## Ejercicio 1

Se sabe que cada vez que un host A quiere iniciar una conexión TCP con B sucede que, en el momento que le llega el primer Syn, B establece otra conexión con un host C, le envía 50 bytes de datos y C le responde 1 byte. A continuación B cierra la conexión de forma abrupta usando un Reset. Finalmente, B continúa la apertura de conexión inicial y sigue normalmente (la comunicación entre B y C es lo suficientemente rápida como para que el Syn de A no genere un timeout).

En un cuarto host D, que se encuentra en la misma red que el host B, se observa la siguiente traza en la que algunos paquetes intermedios no se pudieron capturar:

ORIG	DEST	FLAGS	#SEQ	#ACK	LENGTH
		S	50		0
		S	60		0
		SA	100	61	0
		A	61	101	0
		SA	100	51	0
		A	51	101	0
			51	101	100

- Sabiendo que A necesita enviarle 300 bytes a B en 3 segmentos de 100 bytes cada uno y que el tercero llega con errores. Completar la traza que vería el host D suponiendo que al final de la transmisión de datos, ni A ni B cierran la conexión y ambos hosts quedan en estado ESTABLISHED. Completar cuál es el host de origen y destino de todos los segmentos de la traza. **Nota: Suponer que A, B y C son pares (ip,puerto)**
- Después de un tiempo, A comienza un cierre de conexión y B le reconoce el cierre enviándole un segmento FIN+ACK. Suponiendo que no se pierde ningún segmento, muestre la secuencia de paquetes explicando la secuencia de estados por los que pasa cada extremo desde que comienza el cierre de conexión hasta que ambos extremos llegan al estado CLOSED.

## Ejercicio 2

En la siguiente tabla, se muestran algunas variables que tiene una conexión TCP recién establecida. En dicha conexión el receptor anuncia una *Advertised Window* cada vez más chica hasta que en el 3er RTT, el emisor se ve obligado a frenar el envío de datos. Luego de 1 RTT llegan ACKs anunciando una ventana más grande, lo que hace que, a partir del 4to RTT, la RWND aumente y se mantenga constante.

RTT	SSTHRESH	RWND	Last Bytes Sent	Last Byte ACKed
1	64KB	12KB	4KB	0KB
2	64KB	6KB	10KB	4KB
3	64KB	0KB	10KB	10KB
4	64KB	64KB	...	...
5	...	...	...	...

- Complete los valores de CWND durante los primeros 4 RTTs.



- b. Suponiendo que el emisor necesita enviar un total de 40KB, continúe el valor de las variables del control de congestión del 5to RTT en adelante, suponiendo que si una ráfaga de datos supera los 15KB de datos, la red descarta todos los segmentos y ninguno llega a destino.
- c. (*Conceptual*) Tanto el control de Congestión como el control de Flujo de TCP se realizan a *lazo cerrado*. Explique cómo se implementan las retroalimentaciones de cada sistema de control aclarando de qué tipo son (i.e.: explícitas o implícitas).

### Ejercicio 3

A continuación, se detallan los servicios que tiene una empresa con sus requerimientos de seguridad:

- Un Proxy Web que usan los hosts de la empresa para acceder a sitios Web en Internet.
  - Un DNS resolver para resolver consultas recursivas de toda la empresa.
  - Un Servidor HTTPS que expone una API que debe ser accedida por los clientes de la compañía desde Internet.
  - El Proxy Web y el DNS Resolver son los únicos 2 servicios que pueden iniciar comunicaciones **hacia** Internet.
- a. Dibuje el diagrama de la red, utilizando un firewall stateful para poder garantizar dichos requerimientos usando una DMZ y escriba las reglas del firewall.
  - b. Se necesitan garantizar las propiedades de NO REPUDIO y CONFIDENCIALIDAD sobre los pedidos a la API que realizan los clientes de la compañía, y se dispone de un certificado digital de la compañía, que contiene su clave pública y está firmado por una autoridad certificante mundialmente reconocida (se puede suponer que todos los sistemas operativos vienen con un certificado instalado que tiene la clave pública de esta autoridad certificante). Explique dónde deberían instalarse los certificados digitales y por quién deberían estar firmados de manera que se cumplan las propiedades solicitadas.

### Ejercicio 4

Un usuario lee sus mails con un *user agent* que usa POP3 para descargar mails y nunca borra los correos en el servidor. Además, para mostrar el contenido de un mail en formato HTML usa el protocolo HTTP/1.1 para pedir los recursos. En un momento dado, el usuario actualiza su bandeja de entrada y descarga a su PC su casilla que contiene sólo el siguiente correo:

```
To: cosme@fulanito.com.ar
From: "ofertas@regalos.com.ar" <ofertas@regalos.com.ar>
Reply-to: "no-reply@regalos.com.ar" <no-reply@regalos.com.ar>
Subject: Muchas baratijas muy baratas!
MIME-Version: 1.0
Content-Type: text/html; charset = "iso-8859-1"

<html> <head></head>
<body>
  Cyber Monday!!!
  <br />
  <br />
  <a href="http://ads.regalos.com.ar/comprar.php">Compre mucho!!! Compre! Compre!</a><br />
  <br />
  <br />
</div>
</body>
</html>
```

- a. Suponiendo que la PC del usuario tiene configurado un DNS Resolver que le brinda el proveedor de servicio, describir las consultas DNS que desencadena la visualización del correo, aclarando de qué tipo son. *Asumir que todas las caches están vacías y que hay un Servidor Autoritativo por zona.*
- b. Suponiendo que entre el host del usuario y todos los servidores involucrados, el *RTT* es igual a 100ms y que el contenido de todos los recursos HTTP son lo suficientemente chicos como para enviarse en un sólo segmento TCP ¿Cuánto tiempo tarda cada conexión TCP que establece el *user agent* para descargar y visualizar el mail?



1

NOTA B+

311/27

# FESTINI SANTIAGO

I	A	ORIG	DEST	FLAGS	#SEQ	#ACK	LENGTH
		A	B	S	50		0
		B	C	S	60		0
		C	B	SA	100	61	0
		B	C	A	61	101	0
		B	C		61	101	50
		C	B	A	101	111	1
		B	C	RA	111	102	0
		B	A	SA	100	51	0
		A	B	A	51	101	0
		A	B		51	101	100
		B	A	A	101	151	0
		A	B		151	101	100
		B	A	A	101	251	0
		A	B		251	101	100
		A	B		251	101	100
		B	A	A	101	351	0

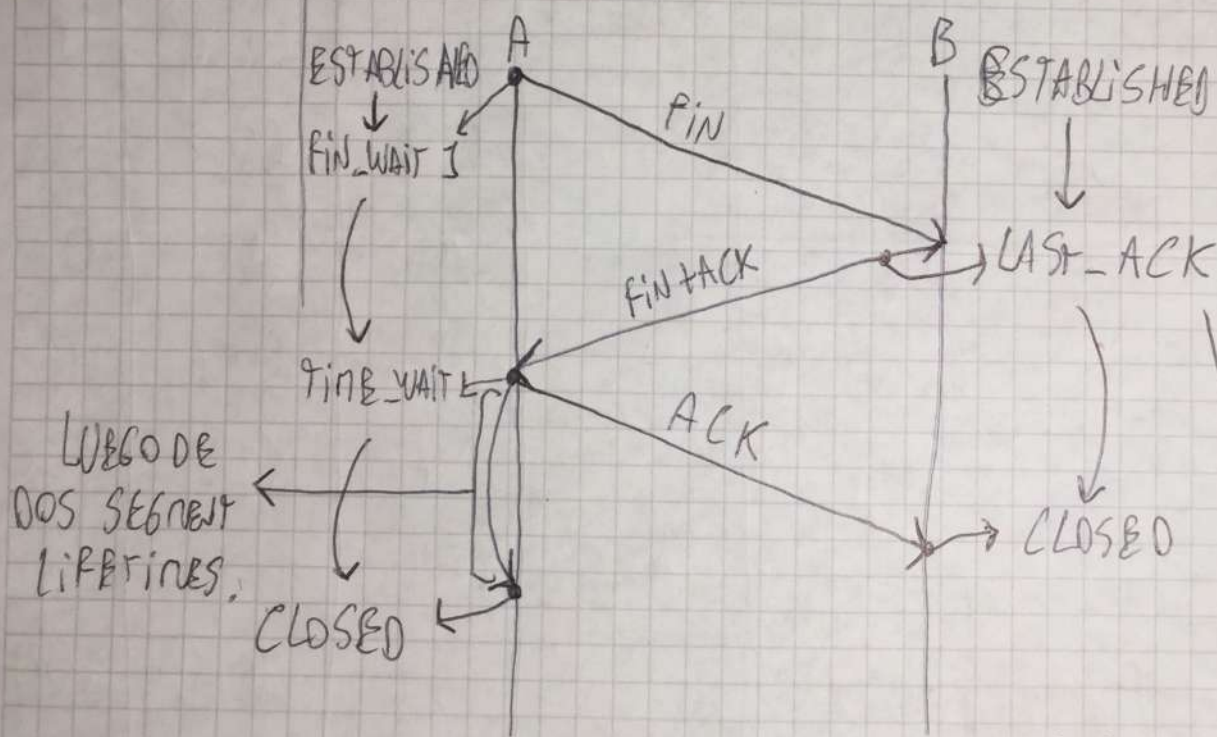
SEGUNTO  
QUE EL  
MAL.  
ILLEGIO  
A

A PARA INDICARLE A

NO ESTOY DEL TDO SEGURO QUE  
ESTO SEA ASI, PERO DE NO SERLO  
ENTONCES B DEBERIA MANOAR  
UN ACK CON #ACK = 251 PARA INDICARLE A

ESTE SEGUNTO  
LEGA CON  
ERRORES POR  
LO QUE B NO  
ENVIA UN ACK  
Y LUEGO DEL  
FINESIT, A LO  
REENVIA!

B	ORIG	DEST	FLAGS	#SEQ	#ACK	LENGTH
	B	A	A	101	351	0
	...	...	...	...	...	...
	A	B	F	351	101	0
	B	A	FA	101	352	0
	A	B	A	352	102	0



ENTENDEO QUE  
 COMO B MANDA EL  
 FLAG FIN JUNTO AL ACK,  
 ESTE SE SALTA EL ESTADO  
 DE CLOSE\_WAIT, YA QUE  
 YA ESTA LISTO PARA  
 CERRAR Y NO DEBE ESPERAR.



(2)

PESSINI SANTIAGO

B=

31/1/27

2.	RTT	CWND	RWND	SS THRESH	Flight size	LBSENT	LBACKED
	1	4 KB	12 KB	64 KB	4 KB	4 KB	0 KB
	2	8 KB	6 KB	64 KB	6 KB	10 KB	4 KB
	3	14 KB	0 KB	64 KB	0 KB	10 KB	10 KB
	4	14 KB	64 KB	64 KB	14 KB	24 KB	10 KB
	5	28 KB	64 KB	64 KB	28 KB	52 KB	24 KB
	6	28 KB	64 KB	64 KB	28 KB	52 KB	24 KB
	7	2 KB	64 KB	14 KB	2 KB	26 KB	24 KB
	8	4 KB	64 KB	14 KB	4 KB	30 KB	26 KB
	9	8 KB	64 KB	14 KB	8 KB	38 KB	30 KB
	10	16 KB	64 KB	14 KB	2 KB	40 KB	38 KB
	11	18 KB	64 KB	14 KB	0 KB	40 KB	40 KB

CONO SOLO  
ES 1 RTT  
DE INACTIVIDAD

→ NO HAY A  
SER LO SUFF.  
PARA GAR.  
IDLE CONNECTION

→ T.O. ←

SE GENERA  
UN TIMEOUT  
PORQUE EL  
RECEPCION  
RECHAZO EL  
SEGUNDO  
TA QUE PESABA  
MÁS DE 15 KB

RTT'S 1-9 → SE UTILIZA SLOW START

RTT-9 : EN EL ENVÍO DEL 4º SEGMENTO SE SUPERA EL SS THRESH POR LO QUE SE PASA A CONGESTION AVOIDANCE

RTT'S 9-11 → SE UTILIZA CONGESTION AVOIDANCE.

\*1: NOTAR QUE AUNQUE LA CWND SEA 16<sup>KB</sup> Y SUPERA 15 KB, CONO SOLO RESTA ENVIAR 2 KB DE DATOS ES NO SE CONGESTIONA LA RED.



C. EL CONTROL DE CONGESTIÓN DE TCP UTILIZA RETROALIMENTACIONES IMPLÍCITAS, SIENDO ESTOS TIMEDOUTS GENERADOS CUANDO SE GENERA UN DESCARTE DE SEGMENTOS POR ESTAR EN UNA RAÍFABA MUY PESADA QUE SUPERA EL NIVEL DE CONGESTIÓN, SE DICE IMPLÍCITA POR QUE EL RECEPTOR NO AVISA ACTIVAMENTE QUE EL SISTEMA SE CONGESTIONA.

POR OTRO LADO, LAS RETROALIMENTACIONES EXPLÍCITAS REQUIEREN UN ROL ACTIVO DEL RECEPTOR, ENCARGADO DE AVISAR A LOS EMISORES EL NIVEL DE CONGESTIÓN DE LA RED Y CUANTO TIENEN PERMITIDO MANDAR, SOFISTICANDO LOS ALGORITMOS Y AGREGANDO COMPLEJIDAD.

Y control de flujo.  $\Rightarrow$

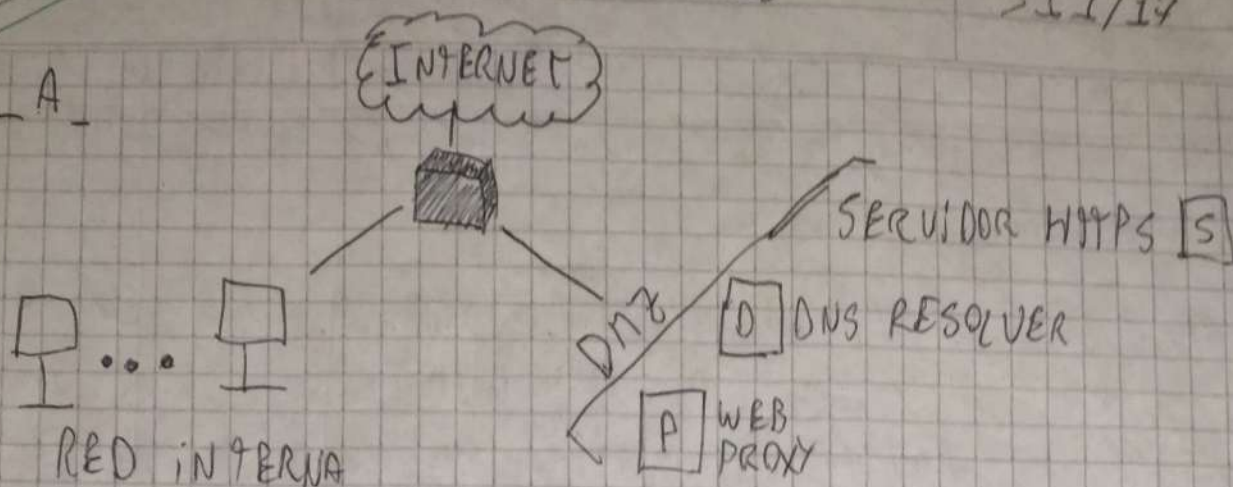
Y otros ejemplos de retro implícitas  $\Rightarrow$

3) Blau+

FESTINI SANTIAGO

3.11/17

3\_A



RED INTERNA → DNS  
RED INTERNA → PROXY

INTERNET → SERVER HTTPS

DMZ → PROXY → INTERNET → HTTP  
DMZ → PROXY → INTERNET → HTTPS

DNS → INTERNET → DNS?

• IMPLEMENTACIÓN REGLAS DEL FIREWALL:

- POLÍTICA POR DEFECTO = DROP.

-  $\langle \text{IP(RED INTERNA)}, X, \text{IP(DNS RESOLVER)}, 53, \text{UDP} \rangle \rightarrow \text{DNS}$

-  $\langle \text{IP(RED INTERNA)}, X, \text{IP(WEB PROXY)}, 8080, \text{TCP} \rangle \rightarrow \text{PROXY}$

-  $\langle \text{IP(INTERNET)}, X, \text{IP(SERVIDOR HTTPS)}, 443, \text{TCP} \rangle \rightarrow \text{HTTPS}$

-  $\langle \text{IP(WEB PROXY)}, X, \text{IP(INTERNET)}, 80, \text{TCP} \rangle \rightarrow \text{HTTP}$

-  $\langle \text{IP(WEB PROXY)}, X, \text{IP(INTERNET)}, 443, \text{TCP} \rangle \rightarrow \text{HTTPS}$

-  $\langle \text{IP(DNS RESOLVER)}, X, \text{IP(INTERNET)}, 53, \text{UDP} \rangle \rightarrow \text{DNS}$



B. ~~NO~~ ~~NECESITA~~ COMO NECESITO CUMPLIR CONFIABILIDAD,  
ENTONCES TANTO EL PROXY COMO EL SERVIDOR DE LA API  
DEBEN POSEER CERTIFICADOS DIGITALES, DE ESTA MANERA  
~~LOS~~ ~~EN~~

PARA LOGRAR CONFIABILIDAD ~~EN~~ LA CONEXIÓN ENTRE  
LOS CLIENTES Y EL SERVIDOR, ENTONCES EL SERVIDOR DEBE  
POSEER UN CERTIFICADO DIGITAL, ~~ASÍ DE ESTA MANERA~~  
DE ESTA MANERA, LOS CLIENTES SABEN QUE EFECTIVAMENTE SE  
ESTÁN COMUNICANDO CON EL SERVIDOR Y NO CON ALGUIEN MÁS,  
Y QUE LA CONEXIÓN ES SEGURA USANDO EL ALGORITMO TLS.  
~~HANDSHAKE~~

POR OTRO LADO, PARA LOGRAR NO REPUDIO, LOS CLIENTES  
DEBEN POSEER CERTIFICADOS DIGITALES FIRMADOS POR EL  
DEL SERVIDOR PARA QUE DE ESTA MANERA EL SERVIDOR  
PUEDA ESTAR SEGURO DE ESTAR HABLANDO CON UNO DE  
SUS CLIENTES Y SABER EXPLICITAMENTE CON CUAL.



4

FESTINI SANTIAGO

31/17



4\_A ASUMO QUE EL CUERPO DEL CORREO YA FUE DESCARGADO, ENTONCES LO RESTANTE PARA LA VISUALIZACION DE ESTE MAIL EN PARTICULAR SERIA LA DESCARGA DE LAS 4 IMAGENES:

- HTTP://ADS.REGALOS.CON.AR/HEADER.PHP?id=OFERTAS 2019

- HTTP://WWW.REGALOS.CON.AR/LINE.JPEG

~~MANEJO DE WWW.~~ → REPETIDA!

- HTTP://ADS.REGALOS.CON.AR/FOOTER.PHP?id=OFERTAS 2019

SE REALIZAN ENTONCES 7 CONSULTAS DNS, 2 RECURSIVAS Y 5 ITERATIVAS

1° RECURSIVA AL RESOLVER → ADS.REGALOS.CON.AR.

1° ITERATIVA, RESOLVER CONSULTA POR AR. <sup>root</sup>

2° ITERATIVA, RESOLVER CONSULTA A AR. POR .CON.

3° ITERATIVA, RESOLVER CONSULTA A CON.AR. POR .REGALOS.

4° ITERATIVA, RESOLVER CONSULTA A REGALOS.CON.AR POR ADS.

2° RECURSIVA, CONSULTA AL RESOLVER POR WWW.REGALOS.CON.AR.

5° ITERATIVA, RESOLVER YA TIENE EL SU CACHA A REGALOS.CON.AR. ES SOLO HACE FALTA CONSULTAR A REGALOS.CON.AR. POR WWW.



B\_ PARA CADA CONEXIÓN TCP, SI O SI DEBO PAGAR  
1 RTT DE SINCRONIZACIÓN  
2 RTT PARA FINALIZAR  
Y 1 RTT POR CADA REQUEST.

⇒ UNA CONEXIÓN CON EL SERVIDOR MAIL PARA REALIZAR  
UN POP3 Y TRAER EL MAIL.  $\approx 4 \text{ RTTS} \approx 400 \text{ ms}$ .

⇒ UNA CONEXIÓN CON WWW.REGALOS.COM.AR PARA ADQUIRIR  
/LINE.SP6  $\approx 4 \text{ RTTS} \approx 400 \text{ ms}$ .

ES COMO ESTAMOS USANDO HTTP.1.1, PUEDO ENTONCES  
REALIZAR VARIOS REQUEST EN UNA MISMA CONEXIÓN.

ENTONCES EN UNA CONEXIÓN CON ADS.REGALOS.COM.AR  
PUEDO PEDIR TANTO /HEADER.PHP?id=OFERTAS 2019,  
COMO /FOOTER.PHP?id=OFERTAS 2019.  $\approx 5 \text{ RTTS} \approx 500 \text{ ms}$ .

EL TIEMPO TOTAL REQUERIDO PARA LAS CONEXIONES TCP,  
NECESARIAS PARA DESCARGAR EL MAIL ES 1300 ms.

